Civilian Research Project
USAWC Fellow

Global Operations and Biometrics: Next Generation Capabilities and Policy Implications

by

Colonel David W. Pendall
United States Army

United States Army War College
Class of 2013

DISTRIBUTION STATEMENT: A
Approved for Public Release
Distribution is Unlimited

This manuscript is submitted in partial fulfillment of the requirements of the U.S. Army War College Fellowship. The views expressed in this student academic research paper are those of the author and do not reflect the official policy or position of the Department of the Army, Department of Defense, or the U.S. Government.

The U.S. Army War College is accredited by the Commission on Higher Education of the Middle States Association of Colleges and Schools, 3624 Market Street, Philadelphia, PA 19104, (215) 662-5606. The Commission on Higher Education is an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.

REPORT DOCUMENTATION PAGE	Form Approved OMB No. 0704-0188

The public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing the burden, to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. **PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.**

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
xx-04-2013	CIVILIAN RESEARCH PROJECT	

4. TITLE AND SUBTITLE
Global Operations and Biometrics: Next Generation Capabilities and Policy Implications

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Colonel David W. Pendall
United States Army

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Mr. Edward C. Wack
Massachusetts Institute of Technology

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
Mr. James W. Shufelt

U.S. Army War College, 122 Forbes Avenue, Carlisle, PA 17013

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT
Distribution A: Approved for Public Release. Distribution is Unlimited.

13. SUPPLEMENTARY NOTES
Word Count: 11,282

14. ABSTRACT

This paper evaluates the current and future state of biometric modalities with application to national security operations on a global basis. The technical evaluations are compared for likelihood of significant breakthrough within the next five to ten years. Next Generation Genomic Analysis, also characterized as Next Generation DNA biometrics, stand out in terms of breakthrough potential in enabling national security operations and countering networked actors and 21st Century security threats. The paper further develops and assesses the breakthrough implications in applied scenarios, or use cases, for national security operations. An evaluation of United States national security policy, presidential directives and law demonstrates a gap in terms of policy scope and applicability to these breakthroughs. The paper provides recommendations to the user and policy community to close these gaps ahead of the coming technology advances in order to ensure the nation's national security posture retains the advantage through use of these capabilities, continuing to ensure the rights, confidences and protections of American Citizens.

15. SUBJECT TERMS
Biometrics, Counter Terrorism, Law Enforcement, Technology, Next Generation DNA

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			19b. TELEPHONE NUMBER *(Include area code)*
UU	UU	UU	UU	54	

USAWC CIVILIAN RESEARCH PROJECT

Global Operations and Biometrics: Next Generation Capabilities and Policy Implications

by

Colonel David W. Pendall
United States Army

Mr. Edward C. Wack
Massachusetts Institute of Technology
Project Adviser

Mr. James W. Shufelt
U.S. Army War College Faculty Mentor

This manuscript is submitted in partial fulfillment of the requirements of the U.S. Army War College Fellowship. The U.S. Army War College is accredited by the Commission on Higher Education of the Middle States Association of Colleges and Schools, 3624 Market Street, Philadelphia, PA 19104, (215) 662-5606. The Commission on Higher Education is an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.

The views expressed in this student academic research paper are those of the author and do not reflect the official policy or position of the Department of the Army, Department of Defense, or the U.S. Government.

U.S. Army War College
CARLISLE BARRACKS, PENNSYLVANIA 17013

Abstract

Title: Global Operations and Biometrics: Next Generation Capabilities and Policy Implications

Report Date: April 2013

Page Count: 54

Word Count: 11,282

Key Terms: Biometrics, Counter Terrorism, Law Enforcement, Technology, Next Generation DNA

Classification: Unclassified

This paper evaluates the current and future state of biometric modalities with application to national security operations on a global basis. The technical evaluations are compared for likelihood of significant breakthrough within the next five to ten years. Next Generation Genomic Analysis, also characterized as Next Generation DNA biometrics, stand out in terms of breakthrough potential in enabling national security operations and countering networked actors and 21st Century security threats. The paper further develops and assesses the breakthrough implications in applied scenarios, or use cases, for national security operations. An evaluation of United States national security policy, presidential directives and law demonstrates a gap in terms of policy scope and applicability to these breakthroughs. The paper provides recommendations to the user and policy community to close these gaps ahead of the coming technology advances in order to ensure the nation's national security posture retains the advantage through use of these capabilities, continuing to ensure the rights, confidences and protections of American Citizens.

Global Operations and Biometrics: Next Generation Capabilities and Policy Implications

Introduction

The United States must maintain a global operating posture to pursue National Security objectives. State and non-state sponsored super-empowered actors continue to threaten the US and our allies by exploiting global infrastructures to move themselves, money, and material resources into positions to act against our national security interests. Advances in biometrics capabilities provide opportunities to resolve identities, to deny anonymity, and alert interagency or partnered foreign law enforcement or intelligence authorities for action as these actors attempt to transit or operate within this global infrastructure.

Biometric capabilities in support of national security continue to improve in terms of speed, variety and specificity.[1] The use of biometrics for security and intelligence has steadily grown in terms of technological capability and variety of modes since 2001. The current field of biometrics contains approximately 200 commercial vendors and is supported by research and development programs in over 40 major universities and US government affiliated laboratories.[2] The estimate for the global investment in all sectors of biometrics from 2012 through 2017 is estimated at US$16.47 billion.[3] The events of 9/11 and the wars in Iraq and Afghanistan fueled much of the sector's investment and its estimate for future investments. Future defense and homeland security related investment spending, as a component of this estimate, is likely to fall significantly due to the ending of the major counterinsurgency operations in Afghanistan and Iraq and the shift in defense priorities.

Austerity will likely force harder choices for continuing DoD research and development investment for biometrics, as biometrics pertain to intelligence and security. In some areas, notably the health industry, research and development efforts by commercial and other USG stakeholders will have benefit to DoD and the overall USG. Deoxyribonucleic Acid (DNA) sequencing advances have fueled wide ranging applications in whole genome analysis for the

health care sector and are beginning to yield insights in the field of bioinformatics. In many cases, specific technological breakthroughs in the field of biometrics will have benefit across multiple segments of the government and civil society. The medical and health industry is continuing to propel advances in DNA genomic processing and information analysis for plant, animal, microbial and human genomes. DNA Sequencing has primarily benefitted the medical and health industries, but could also have powerful applications within the intelligence and law enforcement communities.[4] Without a national security investment in research and development of security related biometric technologies, the US government will not be able to leverage these advances into advantage for US national security in the 21st century. This complementary DoD investment in the applied research, development and technologic integration is required to adapt the commercial and non-DOD DNA genomic sequencing advances for specific DoD and national security related needs.

While this paper reviews and compares the range of biometric sensing and exploitation capabilities, this research focused on identifying the most promising biometric technology for achieving significant advances or "breakthroughs" in the next five years based on current research and development efforts, as expressed by biometric community leaders and subject matter experts in biometric community forums and scientific literature. The identified breakthroughs should be considered in context of their potential impact for use for national security purposes and the range of additional capabilities these breakthroughs may create.

The paper also examines and summarizes US biometrics policy in regard to potential privacy and legal concerns associated with expanded use of current biometric modalities. More importantly, the research reveals gaps in policy or absence of policy that may hinder or set back advances in expanded uses or wholly new methods of biometric collection and exploitation.

These gaps may cause technologic breakthrough or investments in technologic capability to go unused or be shelved due to perceived policy constraints, policy restrictions in investing for applied research, or lag times in policy implementation – each condition would

produce setbacks in biometric application if not coherently addressed. Part of the solution lies in the education of the broader stakeholders and the US public on the safeguards and proper use of biometrics for security and the role of science in providing assured capability and confidence in the modalities.

As the issue of identity, property, privacy and security is becoming even more intertwined, the nature of the threats to the nation is concurrently becoming decentralized, globally and mobile. Threats from Super Empowered Individuals - enabled by a variety of networks - commercial, licit, and illicit, requires a security system commensurately capable of finding and fixing these individuals at the human level, removing their anonymity, with precision and confidence in support of global action.[5] Our security posture and national policy is evolving away from nation state adversaries with large land, sea, and air (and nuclear) forces and shifting increasingly toward the non-nation state actors organized as networked violent extremists, often seeking weapons of mass destruction. We have begun to understand the need to pursue methods that allow the US and other nation security systems to pursue these threats by basis of individual identification with confidence.

This paper will conclude with recommendations for changes to current policies to ensure technologic capabilities are understood and leveraged to support the nation's security posture in the 21st century.

Approach to the research

The research efforts supporting the findings in this paper rely heavily on the scientific community and the research and development community insights as communicated through briefings, subject matter expert interviews and technology reviews. In short, it is a technology and policy evaluative approach, with prescriptive recommendations to best ensure advances in technology are supported by policy in the operational environment.

The overall methodology identifies those biometric modalities which are most likely to have breakthrough advances over the next five to ten years, reviews the types of advances, and

discusses why they are relevant to the national security stakeholders. Modalities as expressed in this paper refer to the broad categories of biometric capability, namely iris and retinal, DNA, fingerprint, voice and face.[6] It then evaluates the current policies and social issues impacting on the modality, extrapolating the impact its breakthrough capability in terms of further friction with existing policies and law.

This paper focuses on the capability to exploit a collected biometric in new, novel, or wholly different ways, as a biometric modality; in short- technologic breakthroughs. The paper does not address other types of advances, such as better integration, data sharing, standardization, or improved collection techniques. Though advances in these areas are important and have impact on the overall usage or value of the biometric to the user community, they do not generally impact on the state of policy and social concern, given that these typically incremental improvements do not fundamentally alter the modality's existing policy position.

In terms of modality advances illuminated through research, the Next Generation DNA (NGDNA) programs, also referred to as Next Generation Genome Analysis (NGGA) have the highest potential for creating significant new policy issues. Breakthroughs in DNA sequencing of forensic samples are likely, and the potential ability to provide characterization of individuals, and possibly their activities, will generate friction in the policy and privacy arena. Some of the envisioned capabilities include mixture analysis, phenotype analysis (which could produce computer generated likenesses or rudimentary "digital sketches of suspects), extended kinship analysis (to develop network diagrams and models based on link analysis and familial support structures) and bio-geographic ancestry characterizations. Current policy does not directly address the use of the breakthrough exploitation capability derived from Next Generation DNA processing and analysis.

Research Paper: Summarized Outline

Section one provides a review of the current biometric modalities and their common use, a prognosis for incremental advances within the modality as well as anticipated

breakthroughs in capability and a crosswalk of the modality to policy or privacy related issues specific to the modality. This section also includes a reference chart on page 13, developed to guide the data collection and capture Modality, Level of Technological Progress, Operational Application, and Level of Policy/Stakeholder Conflict with a common coding for evaluation.

Section two is a summarized review of current policy, legal and privacy issues related to current biometric use of the DNA analysis. The section also introduces projected policy gaps and identifies the absence of policy in terms of the Next Generation DNA advances.

Section three provides discussion and review of the current security related concepts incorporating the DNA analysis. A series of vignettes, or use cases, incorporating the projected advances in the DNA analysis provides the main argument as to why DNA related advances have the most potential for enhancing national security. Further, the use cases serve to illustrate why the DOD and other National Security Stakeholders should maintain investment in the DNA modality to realize and implement these potential advances in the next five to ten years. Additionally, the section also discusses the concept of security as it relates to the requirement to pursue threats from the Super Empowered Individuals and their networks, which differs from the security paradigm focused on State on State conflict and conventional military confrontation. Increased resolution of the threats challenging the nation's security will require assured identification to the individual level.

Section four provides prescriptive policy adjustment recommendations to fully leverage future biometric capabilities while addressing stakeholder perspectives and concerns. The section also makes suggestions for all stakeholders in terms of education and training related to DNA-based biometrics.

Section five provides an overall summary and conclusion of the paper. This section also briefly addresses some key trends and indicators of the future state of biometric technologies beyond the 10 year mark.

Section One- Overview and Evaluation of Biometric Modalities

At its core, the basis of biometrics is rooted in statistical probability. The collected sample is documented, analyzed and stored in a database in digital form. A computer runs a matching algorithm to identify any previously collected samples that "match" based on a statistical likelihood that the samples are from the same individual. The operative presumption is that all individuals have distinctive characteristics that allow others to determine that you are you and someone else is "not you" and vice versa.[7]

Some biometric methodologies, or modalities, are likely to produce a higher average of statistically reliable match, and others are more likely to have a lower average rate, with a higher chance of false positive or false negative. For example, biometric modalities involving DNA have the highest confidence rating (higher than 99.999%) than other biometric modalities such as iris and fingerprints.[8]

Other factors that are important for biometrics as a national security tool are the ease of collection, whether forensically or "in person." To be sure, there is no "best biometric," in terms of ease of application, operational context and conditions or overall cost (resources and time). When possible, especially in a law enforcement or intelligence related use, the preference is to obtain multiple biometrics from the same individual or group of individuals (or crime/event scene).[9] Some collection methods require physical contact with the individual or the individual's biologic residue, and others can work at a distance from the subject, determined by operational conditions and sensitivity of the collection device. Some biometric systems, known as "soft biometrics," are based on behaviors such as handwriting, "walking gait," and even computer keystroke patterns, or some physical features such as scars or tattoos, and are not fully capable of reaching confidence levels that are commensurate with actual match and individual identification.

Some biometric modalities have a higher perception of being "invasive" and/or related to a "Big Brother" surveillance system that opponents claim infringe upon one's privacy or civil

rights and allege the trampling illegal search and seizure laws. Examples of higher societal friction modalities include facial recognition, iris, DNA, as compared with less contentious modalities which are not popularly perceived as outside the norm in most societies, such as fingerprints, and voice.

In assessing the range of capabilities desirable across the modalities for a biometric collection and exploitation system in support of global national security operations, there are a few core elements that emerge:[10]

- the capability to leverage Non-Contact/Stand-Off collection techniques;[11]
- the capability to collect on Uncooperative, Non-Cooperative, and Cooperative persons of interest;[12]
- the capability to discern individual attributes from within messy conditions (non-lab or uncontrolled field environments);[13]
- the capability to conduct rapid forward exploitation with minimal training;[14]
- the capability to ingest/upload digital biometric data into enterprise data systems across commercial or military digital communications means;[15]
- the capability to match a reference sample with a stored database sample of the individual (1:1), match a reference sample with a known or unknown individual (1:N matching), and match an unknown sample with a dataset of other known and unknown data (N:N matching);[16]
- the capability to extract information from forensic evidence and generate intelligence leads on unknown individuals and individuals with no previous biometric enrollment.[17]

Summarized Evaluation of the Modalities

The following summarized evaluations are based on the totality of the research conducted in producing this paper and incorporates technical briefings, subject matter

interviews, and literature reviews.[18] The primary modality evaluations are presented in alphabetical order for ease of reference and do not indicate a prioritized "best biometric" list.[19] Several other biometric modalities in common use today, such as those used for individual authentication for access to accounts or facilities, are not included in this evaluation due to their limitations in application to current or future national security use cases (additional rationale is offered in the endnote).[20]

DNA. DNA has been a commonly used biometric since the mid 1980s and has wide use in criminal forensics to identify suspect "donors" from hair, blood, semen, saliva, or skin flakes remaining at crime scenes (latent DNA samples).[21] The primary DNA modality used to analyze a sample is the Short Tandem Repeat (STR) process, which replicates the DNA in the sample into an amount sufficient to reveal the STR coding unique to a single individual's genome.[22] The other collection method for a DNA sample is considered active or "invasive," which is done by collecting a DNA sample via cheek swab, blood, or saliva directly from the donor (reference DNA samples). DNA STR analysis supports identity resolution and is regularly used for first generation familial heritage (parent-sibling or immediate family).[23]

Progressing from the current use of DNA Short Tandem Repeat (STR) matching, the emerging NG DNA Sequencing capability enables numerous additional opportunities for analytic exploitation.[24] The NG DNA focuses on specific coding within the DNA and moves beyond non-coding genome analysis for identity verification to evaluation of the coding region genomes using Single Nucleotide Polymorphisms (SNP) sequencing analysis. Genomic sequencing techniques could soon enable multi-donor identification and intelligence lead generation, bio-geographic ancestry, activity based analysis from changes resident in genetic makers and microbial cells co-present with the human DNA, and extended kinship analysis. It may also provide the capability to generate facial and physical feature "likeness" creation based on genome markers in the future.[25]

The uses of DNA for national security, particularly in a counter-terrorism role are significant. DNA can be used for identity resolution of individuals connected to terrorism events, confirm identities of High Value Targets and detainees and support screening of visa applicants for amnesty programs through kinship analysis. It can be incorporated into focused enrollment operations for screening against previously collected forensic samples where suspects were listed as unknown, as well as advanced analytics to establish tangible leads on non-enrolled, unknown individuals. Each of these advanced applications has policy implications, civil liberty and ethical concerns.

Face. Facial recognition is arguably the oldest form of human identity resolution. Rather than humans looking at other humans to determine "who is who," computer algorithms search digitized features of facial images captured in a variety of modes - close, at standoff, etc. The technology for processing facial images and the crosschecking algorithms, while improving, are not likely to be measurably different in kind over the next five years. Although social media sites like Facebook© use a type of facial recognition for "find friends" and "friend tagging" in uploaded image content, the use of facial recognition by the USG Government, especially when captured via street cameras and Closed Caption TV (CCTV) and then stored/retained, remains less accepted. More broadly, there are concerns of privacy and individual rights when the widespread use of facial image capture and long term database storage is discussed, even though facial photography is the norm for government and state identification cards and has been for generations. Many of these government use potential examples are restricted in terms of image capture and long term database storage by policy and law, specifically in order to protect individual privacy and civil liberties.

The technologic advances which move the capability from recognition into actual identity confirmation (facial identification and verification) are improving, but remain limited by distance, camera angle, image quality, and reference image to collected image comparative matching. As a Law Enforcement or Intelligence "lead" generating modality, the facial recognition and

identification modality remains of high value. Lead generation establishes tips and clues for intelligence and law enforcement professionals to follow, rather than narrowly focusing on establishing evidence for prosecution. The value of extracting facial features from two-dimensional (2D) and three-dimensional (3D) image collection will improve as software improvements are applied to high definition still and video imagery. This area of modality enhancement will likely take advantage of the enormous expansion of everyday "collection" and posting of pictures and video on the World Wide Web, via social media, international news footage and commercial or homemade video postings.

Fingerprint. Fingerprints are the oldest modality in use today for law enforcement, identity resolution, forensic evidence for criminal prosecution and intelligence use. Fingerprints are used worldwide and technologies have moved from analog (inked fingerprints on cards/paper) to digital (optically scanned fingerprints stored as a unique feature file).[26] Collection techniques obtaining fingerprints from the individual (alive or dead) through collection device contact with the fingers is the norm. Fingerprints from forensic collection ("dusting," tape lift and use of vapors to reveal fingerprints) are widely used as evidence in criminal cases to confirm suspects against the print (1:1 match, 1:N match). Fingerprint biometrics are also the internationally accepted norm in US Immigration and Visa identity verification at US ports of entry under the Homeland Security US-VISIT program. Visitors are required to submit to a 10 fingerprint scan and full frontal facial two-dimensional photograph for automated check within the US immigration database and the FBIs IAFIS fingerprint database.[27] There are some devices being developed in the commercial sector with potential application to Homeland Security, Law Enforcement and Intelligence that allow for the collection device to leverage noncontact, proximity scanning technologies.

Based on literature review and interviews with respected subject matter experts in the biometric community, there may be a few incremental improvements in fingerprint collection and biometric fingerprint science but there are no significant new breakthroughs expected in thie

modality over the next five years. Current policies are sufficient and support current use cases and foreseeable incremental improvements in fingerprint based biometrics for national security purposes (identity verification and intelligence).

Iris (and Retina). Both modalities are very viable for identity resolution in a law enforcement and intelligence role. The error rates are low and the ease of use allows new users to employ the technology with minimal training. The industry has supported commercial and government requirements, for identity resolution and for access control in some higher security level facilities. Iris collection (the colored portion of the eye) is viewed as less intrusive than retinal scanning (the back of the eyeball). Some recent research indicates that the iris is subject to change over time due to the human aging process, calling into question the permanence of this biometric.[28] In terms of collection and exploitation advancements, there are some efforts to increase the distance in which a viable iris capture could occur with changes in optics and focal plane technologies, with a view to create a viable standoff capability for iris collection in support of law enforcement and intelligence operations.

At this point, a review of the literature, basic and applied research efforts and dialogue with subject matter experts, there is little promise in more than incremental advancements in this modality. Primary limitations remain the inability to cope with non-cooperative or uncooperative subjects, distance, and image angle.

Voice. Improvement in voice identification technologies continues steadily as commercial application for access control (increasingly used in phone based voice recognition and account access applications) drives some commercial activity. Voice recognition (defined here as computer-based recognition of the spoken word, such as automated menu features in telephone customer service options) is different than the biometric modality of Speaker Identification or Authentication (actual attempts to confirm a 1:1 person match with a previously collected sample from the same individual). The challenges within speaker identification and authentication, as a true biometric, remain with the circumstances of voice collection and with

the physiological condition or health of the subject. In terms of circumstances of collection, the voice sample quality is affected by background noise, sample length, quality of the collection means (digital or tape recording or over radio, television, through a phone). With physiology and physical health, the speaker's voice can change between time of sample and the reference for match, especially if the individual is sick, highly stressed, or using a dialect or changes speech pattern due to differences in the social relationship and context of the interaction).[29] Thus, matching in a 1:1, N: 1 or 1: N scenario remains difficult and subject to legal challenge in many cases. Nonetheless, as a lead generation and intelligence or law enforcement tool, even without certainty of identity, voice remains a modality with high value. In most law enforcement and intelligence scenarios, the utility of voice collection is likely to be more focused on the internal content of the message or communication event itself than necessarily on the speaker identification.

The value on speaker identification as a biometric tool is primarily for high profile criminal cases or high value individuals for intelligence purposes. For these reasons, voice collection and the use of collected voice is addressed in US law, domestically and in overseas circumstances. Under Title 18 US Code (Title 18 USC) and under the 1978 Foreign Intelligence Surveillance Act (FISA), and under the Uniting (and) Strengthening America (by) Providing Appropriate Tools Required (to) Intercept (and) Obstruct Terrorism Act of 2001 (commonly known as the PATRIOT Act), procedures for lawful collection of voice for use by US Government entities (requiring a warrant to collect), retention and the sharing of that collection is addressed. This is particularly pertinent in terms of Search and Seizure law derived from the 4th Amendment of the US Constitution, which addresses the use of covert collection ("wires" or microphones), wiretaps, and wireless collection means against criminal suspects and intelligence targets. This is especially the case when concerning US Citizens and US Persons domestically and overseas, as differentiated from foreign persons overseas. In summary, voice collection as a biometric tends to generate the most scrutiny and concern of privacy and rights

violations of the primary biometric modalities currently in common use. As such, the US Government has instituted oversight and legal statutes to regulate and monitor related uses of this modality, while recognizing its significant contribution to national security and criminal prosecution.

Table: Summary of Biometric Modalities and Qualities[30]

Modality	Overall Confidence Rating of Modality	Incremental Enhancement or Breakthrough?	Application Understood	Enabling Policy	Policy change?	Modality stress in terms of social/legal/political concerns
What is it?	Prosecution? OCONUS Counter-Terrorism? Access to restricted areas/data? Point of Entry (POE) Identy Confirmation?	In the next five years, is there an expected **Incremental advance** in confirmation or collection technologies or **Breakthrough**?	Community of Practice (CoP) is ready to integrate enhancement or breakthrough- clear practicioner readiness to implement enhancement or breakthrough	Policy supportive of incremental improvement. Policy supportive of breakthrough without change.	Required Policy Change or Development of new policy required to accommodate new capability?	Will this enhancement or breakthrough trigger opposition and pushback? By who? What has this modality experienced so far in terms of scrutiny or opposition? Will the enhancement receive same or different concern? Why?
Iris	High	Incremental	Understood	Adequate	No	No
Retina	High	Incremental	Understood	Adequate	No	No
DNA	High	**Breakthrough** NGGA- SNP Genome Analysis/ Epigenome Analysis/ Mix Analysis/ BioGeographics/ Extended Kinship	New Use Cases	Gap	Yes	Yes (See Section 2, 3, 4 for review and recommendations)
Fingerprint	Moderate/High	Incremental	Understood	Adequate	No	No
Voice	Moderate/Low	Incremental	Understood	Adequate	No	Challenges, USC 18 for Surviellance addresses this issue//Also PATRIOT ACT and FISA
Facial	Low	Incremental	Understood	Adequate	No	Challenges from Privacy Advocates on collection and storage of CCTV and public camera imagery

In summary, this research finds that DNA is the leading modality for the precision and confidence in the identification of individuals connected to violent extremist organizations and terrorism. It has the highest likelihood of breakthrough capability and is enhanced by the progress to reduce cost and processing time and to improve ease of use across the user community.

Section Two- Policy, Law, and Privacy Issues

In order to fully leverage the scientific and technological advances emanating from the Human Genome Project, concerns should be addressed in the areas of privacy, policy and

lawful use of derived biometric information.[31] These capabilities offer great opportunity to impact the national security posture for the nation. Currently, the broader application of biometric use and sharing for national security is governed by National Security Presidential Directive 59 and Homeland Security Presidential Directive 24 (NSPD 59/HSPD 24), which was established following the al Qaeda attacks of September 11, 2001. This dual directive, under subject header "Biometrics for Identification and Screening to Enhance National Security," established the framework for federal executive departments and agencies to share and exchange biometric and related biographical information. The directives addressed the biometric enrollment of individuals in a lawful manner, while respecting their information privacy and other legal rights under US law.[32] Even before NSPD 59/HSPD 24 was established in 2008, the recognition of the need to coordinate federal agencies and sharing was codified in 2003 under HSPD 6 (Integration of Screening Information). This established the Terrorist Threat Integration Center, now called the National Counter Terrorist Center (NCTC). In 2004, HSPD 11 (Comprehensive Terrorist-Related Screening Procedures) implemented a coordinated and comprehensive approach to terrorist related screening in the US and abroad, building upon HSPD 6. These three HSPDs, as well as the 2005 Executive Order 13388 (Further Strengthening the Sharing of Terrorist Information to Protect Americans), cover the Presidential Directives establishing policy on the use of biometrics for national security related activities.[33] The documents do not specifically cover DNA as a biometric, although the intent of the policy and directives clearly establish the need to pursue biometric capability and leverage their use within the scope of national security. Though armed with the intent of these directives and orders, the pursuit of Next Generation Genomic Analysis capabilities should advance with a solid concept of operational use and a recognition that moving from identity resolution from DNA STR matching across the 13 loci (FBI standard for identity confirmation) significantly changes the dimensions of the exploitation value and raises concern for misuse when exposing the underlying genomic information found within the DNA sample.

Other national security policy and law centering on coordination and operations of our federal agencies for the protection of the US homeland also lack specific direction or guidance on the issue of DNA and genetic information within the context of national security requirements. The PATRIOT Act is comprehensive in pulling previously disparate laws together with a view to create better coordination, cooperation and sharing of national security and terror related information across the federal government. It specifically addresses collection and surveillance legal authority for the FBI, CIA, NSA and capabilities from other US security agencies. Subordinated under the PATRIOT Act, The Foreign Intelligence Surveillance Act and the Title 18 USC address US citizens and US persons (persons legally within the US or affiliated with US Corporations and protected by US laws as pertaining to intelligence collection) with respect to the collection and storage of personal information. Under Title V of the PATRIOT Act, the use and storage of DNA is addressed under the DNA Analysis Backlog Elimination Act of 2000, which authorized states to use and input DNA samples from criminal cases and charged individuals into the FBIs CODIS database. Section 503 of the PATRIOT Act amended and broadened the DNA Analysis Backlog Elimination Act to provide for the ingestion of DNA collected from investigations of acts of terrorism and terrorist related events, as they are considered qualified federal offenses.[34] While the Act does not account for expanded or Next Generation DNA information (SNP and genomic information), importantly, the Act does provide for criminal penalty against individuals who improperly disclose sample results or improperly obtain or use DNA samples.[35]

Primary policy-related concerns to the advances in DNA genomic exploitation are addressed under US law in the context of medical use and health care/medical insurance concerns through the Health Insurance Portability and Accountability Act (HIPAA) and the Genetic Information Nondiscrimination Act (GINA).[36] Both Acts cover the inclusion of technologies to expose underlying personal and genetic information from patients or citizens, establishing intended safeguards against misuse of the information, such as denial of coverage

or predatory business practices against persons identified through genetic testing as having certain diseases or hereditary predisposition for specific health issues. These acts do not cover issues of DNA related biometrics for national security use, although the potential for intentional or inadvertent cross-correlation between health industry data and DNA samples in national security datasets should not be discounted. This potential or concern is also true when considering the capability to move into lead generation when attempting link analysis and network development activities, as extended kinship analysis and even surname analysis may offer investigators another avenue for exploitation.

The primary issue with DNA collection and retention in terms of law and privacy is related to a US Citizen's Fourth Amendment Rights, but these generally do not apply when collecting samples or forensic evidence overseas or from crime scenes inside the United States.[37] Additional concerns could also be raised regarding the informatization of the body and the ability for genomic information to be collected and the information would "testify," against an individual without consent, violating a person's Fifth Amendment rights against self incrimination. In a RAND Occasional Paper "DNA as Part of Identity Management for the Department of Defense," the author states "In general, few legal impediments stand in the way of DoD's use of DNA for identification in overseas military operations, but DoD still needs to be prepared…"[38] The RAND paper's author further advances the thought of future DNA collection and use within context of national security and DoD intelligence by offering that the framework for overseas use be divided into two categories: Combat Zones and Other Areas.[39]

In terms of Combat Zone collection and use, DoD has maintained the accepted practice of collecting DNA from IED related events and some Sensitive Site Exploitation in Afghanistan and Iraq, but the larger questions about bi-lateral or multi-lateral sharing DNA profiles with foreign governments remain. Currently, DNA profiles of foreign persons involved in security related incidents or checks, foreign persons requiring access to US installations in combat zones as workforce or regular visitors, an overseas forensic DNA collections do enter the US

Government's primary DNA database, maintained by the Federal Bureau of Investigation- the Combined DNA Index System (CODIS). These overseas captures and enrollments were and are done with the full acceptance of the host nation governments. In the case of Afghanistan, the Afghan National Security Forces and courts also support US and Coalition enrollment and use efforts as a broader program of security and counter terrorism.[40]

As for DNA collection operations in non-combat zones overseas, and "Other Areas," the full scope of applicability for covert DoD and non-DoD intelligence operations remain viable. To be sure, the collection, processing, analysis and storage of DNA derived information are focused on non-US individuals in overseas security and intelligence operations. As the RAND occasional paper points out, however, there would likely be limits for collection within specific countries that the US maintains intelligence cooperation with, and there would likely be agreed to limits on intelligence on host country nationals.[41] Each nation would likely require a bi-lateral agreement for USG DNA biometric reference sample and latent sample collection within its borders, and most likely this would occur in conjunction with their own law enforcement or security service operations. The Other Area operations where there is a value in collecting DNA either forensically, covertly or actively (in person) should also be addressed under US Policy, extending the potential for combined law enforcement or security service operations with US interagency teams (CIA, FBI or DoD), as these capabilities benefit the partner nation and the US in terms of counter-terrorism and threat network development. The questions to be addressed are related to sharing, whether it is sharing of DNA profiles, access to datasets/databases, or the actual DNA samples.

Policy gaps on the use of DNA for intelligence and identity resolution of potential or suspected terrorists, as well as other hostile state and non-state actors remains insufficiently developed when considering the need to collect and store DNA from forensic investigation. Concerns directly related to the collection and use of DNA information derived from Next Generation capability (SNP and broader genomic variant types) are raised as the capability

moves from identity resolution (confirming a person's identity or involvement with an event or incident through forensics through DNA STR match) to the exploitation of a person's genome structure and actual genetic code, which moves well beyond identity resolution.

Though SNP analysis, one's genome can be analyzed to reveal tribal or clan relationships, susceptibility to disease, the bio-geographic correlation to specific regions and sub regions of the world, visible physical characteristics from genetic markers (phenotype analysis) determination of co-presence of microbial DNA (metagenomes), extended kinship, and even surname prediction. DNA could eventually reveal probabilities for recent locations, travel history, handling of toxic materials, etc. Information stored and or shared with other nations could result in misuse, even if the USG implements controls and safeguards for the use of this DNA information. Even with this risk, the value in exploiting the potential intelligence derived from SNP analysis is clear, as the ability to further deny anonymity, association, activity and network affiliation comes into being.

Another feature of NGGA/NG DNA is the ability to perform meaningful sample mixture analysis. Science shows there is a reliable process for taking touch sample from common objects and determining how many different individuals have had contact with the object. Literally, how many people have been through the doorway (touching a doorknob) or as a law enforcement and security example, how many people have handled a gang or terrorist weapon and whether or not a specific individual is included in the mixture?

Section Three- Next Generation Genomic Analysis Use Cases and Potential Future Concepts

The current and future use of DNA biometrics offer a great advancement in resolving identity and creating intelligence lead generation for countering super-empowered individuals and their networks in the 21st century. This section addresses the current and future scenarios where DNA biometrics are being applied or could be applied for national security. This review will cover the current STR based use of DNA biometrics, advancements and forecasted

advancements in the DNA STR processes and remaining shortfalls in these approaches. Secondly, the breakthroughs in SNP genomic information exploitation are examined as potential use cases for national security which could be applied to combat terrorism, weapon of mass destruction trafficking and offer intelligence lead generation for global operations. Finally, the section discusses the role of identity, the nature of the 21st century threat and provides the case for investment in next generation DNA capability as another important tool for the nation's security.

DNA STR applications in National Security

The first application of DNA STR analysis as changed by technological breakthrough is the ability to conduct forward (non-lab) processing of DNA samples within a single device.[42] The breakthroughs associated with Rapid DNA technologies can soon enable field operators to collect and analyze DNA and have results of match against the CODIS dataset or the ability to generate DNA digital files for ingestion to CODIS in under 1.5 hours (swab to digital STR result). Prior to this breakthrough, DNA STR analysis had to be conducted under lab conditions, and each step of the process, from PCR replication, to extraction and coding, to full readout, required separate devices for each step and trained lab technicians for each step. With the process enabling technology, multiple samples can be analyzed and results checked against the DNA repository by field agents, rather than technicians, and under basic field conditions (non-lab conditions, limited climate control, and with limited power supply). Timeliness matters for operations, as the cycle times for analysis must support the operational timelines and requirements for action. As an example, Rapid DNA timeliness allows for results feedback while detainees are present or while an event scene is still under security control/lockdown. The prognosis for even faster sample scan to readout rate is positive, and we should expect sample to result cycle times in well under one hour. Current rapid DNA processes are dependent on buccal cell swabs. Future advances should allow for samples of less than one nanogram (about a hundred skin/fluid cells, or the amount of DNA material left behind from

touching or handling objects). Additional research and development will also take the device size from the current table top device (size of a large color printer) to that of a handheld device (shoebox size or large laptop sized device). Further, costs have rapidly declined, with the cost for a 13 loci DNA STR sample analysis expected to be below $100.00/sample in the next five years. In summary, the previously held detractors for the viability of forward DNA biometric collection and analysis, namely cost, complexity, and speed have been eliminated and opportunities for new uses abound.

Forward Rapid STR DNA Biometric Use Cases:

- **Incident witness and suspect enrollment, forensic exploitation and match.** Give a terrorist, security or significant criminal event, Rapid STR analysis could run concurrently with STR samples and processing from individuals retained or detained on site as security teams and forensic teams conduct site exploitation for trace elements of chemicals, explosives, latent prints, trace DNA, etc. The benefit is an established, undeniable record of presence within vicinity of the event location and the ability to match any previously enrolled (watchlisted) individuals, cross check with forensically derived DNA from the incident itself, and also allow for the ingest of suspected but released individuals associated with the event.[43] In this use case scenario, and those that follow when referring to Rapid STR DNA processing and analysis, one expectation is that the development of rapid PCR (DNA generation through chemical replication from sample) is also concurrent, especially for deriving STR samples forensically.
- **Border screening and immigrant analysis.** Incidents related to the detention and screening of illegal immigrants arrested at illegal border crossings can now be processed for DNA enrollment and match very early in the detention process, allowing for a much richer review of the individuals biometric history and also cross check with other forensic datasets, derived from other nation collection (if

biometric sharing agreements are in place) and allow for a near immediate check of the individual against other incidents or security related events. This has a wide range of counter-network application, for the US and North American neighboring countries, as well as partner nations around the world. Additionally, specific use in combating Weapon of Mass Destruction (WMD) component trafficking, Drug and Weapon Trafficking, and Human Smuggling can be realized.

- **Watchlist screening.** A wide range of screening and verification programs could be augmented by Rapid DNA STR analysis, especially in remote areas and locations with limited infrastructure. Though many watchlisted individuals have biometric enrollment (usually face photograph, fingerprints, and often iris), the use of DNA STR capability opens the opportunity to match against forensically derived DNA evidence, using something with a higher confidence than latent fingerprints, particularly from national security incidents and sensitive site exploitations in combat theaters and other overseas locations.
- **Maritime Interdiction and Screening.** Open sea interdiction of vessels, particularly in checks of suspected piracy related vessels and crews, vessels suspected smuggling embargoed or other illicit materials, and other suspected state or non-state trafficking platforms, the DNA processing for match or the initial enrollment would establish true biometric identity in databases and allow for the cross-confirmation from other biometrics or biographical files on known or unknown individuals. Further, the forensic processing opportunities onboard ships and with cargo also provide a richer dataset for threat or illicit network analysis and development.
- **US and Partner Nation security force verification.** Rapid DNA STR enrollment and processing will also serve the identity verification and partnering of coalition military and security operations, moving beyond identification cards,

fingerprint authentication or iris scan verification. With the DNA STR coding, the full record can be established and act to fully confirm partners involved in sensitive or high risk joint and combined operations.

Next Generation DNA SNP applications in National Security.[44] A next Generation DNA capability essentially means that the processing of DNA moves into the DNA makeup at the genome level. Fundamentally, this changes the DNA modality from one of analyzing a limited set of identity markers through STR analysis, to "informatization" the body and providing a wide range of operationally useful information from the broader genomic DNA analysis.[45] Said a different way, the breakthroughs allow any genomic code to be de-coded and turned into a machine-readable dataset. From this conversion, a digital pattern is established for each sample (think individual genomic blueprints converted into a "barcode"). That barcode can then be comparison matched in a variety of ways, including base type characterization, visual representation of major characteristics, references against other "like" genomes, pattern matched for conformity with biologic-geographic ancestry, ethnic and familial traits, and also for differentiation in extremely small sample sizes derived from forensic mixtures found in publics spaces or at security related sites or events. Given the progress on the ability to generate vast amounts of information content from sequencing of the human genome, the national security information architecture should be readied for the need to ingest, store, cross reference and share these new sources of intelligence and national security related data. Current biometric systems all suffer, from one extent to another, from the non-integrated, non-standardized and ungoverned development of local systems and data formats resulting from commercial vendor developed tools and technical protocols.

Cost factors for DNA SNP scans in commercial and health industry sectors are dropping significantly as well, with initial (early 2000s) were over $10,000 per sample analysis, and recent commercial advertisements for personal scans have the prices for individual purchases below $400.[46] Some estimates place the coming cost per sample run below $50.[47] Bioinformatics

development for disease and overall genomic health characteristics contained in the genome patterns, be they plant, animal or human, is driving the cost factors down as new processor chips, nanoscale technologies and distributed parallel (cloud based) computing power are applied to the genomic science. There are cost differing cost variables based on the types of sequencing scans and chips used to generate specific types of genomic information, but the point is that processing costs are all rapidly declining. Bioinformatics and the whole genome scientific revolution is clearly an area where the national security application and opportunities are advanced due to civil and commercial research and development.[48] With proper policy, oversight, education and balanced approaches to proper use, these advances can be brought to bear on the nation's national security challenges.

Assessment of Technical Readiness for Application to National Security. The following NGGA/NG DNA emerging capabilities are in order of relative technical maturity for potential application.

The first application for DNA SNP exploitation is **mixture analysis**. Mixture Analysis represents a breakthrough capability in its own right, allowing high probability discernment of individual involvement in an event or association with object through DNA sample analysis. One of the problems in DNA STR analysis with the 13 or 16 standard genomic loci is that though identity could be established with virtual certainty, it also required a fairly straightforward forensic sampling. With a one nanogram sample of DNA, (or even lower amounts in some cases), collected from items or surfaces, the DNA sequence processing techniques produce certainty as to the contributor. When the sample contains a mix of DNA, containing mixtures of multiple STR and SNP evidence, the results are inconclusive.

With mixture analysis, drawing on clues from the SNP based genomic markers, the ability to confirm an individual against the mixture is now possible. In the current state of the science, a reference sample (known) can be compared against a mixture of up to eight unknown donors. Current laboratory testing demonstrates the consistent ability to confirm the

presence of match with reference samples against up to eight different donors from touch samples at less than one nanogram of material per donor. Additionally, the mixture analysis technique is being tested against an even greater number of DNA donor mixtures, perhaps reaching the capability to identify single individuals from mixtures containing upwards of 100 different persons.[49] Said another way, the current processing techniques can confirm if the reference profile is present in the mixture, or not (1:N match). In the future, the follow on capability could actually isolate individual DNA markers from a mixture of donors, a process called deconvolution, allowing for full identification of donors in a mixture or allowing the DNA to be separated and uploaded as unknown individuals but specified as identified genomic profiles. In the advanced case, this would allow for N:1 and N:N matching.

The second application is the SNP exploitation for **extended kinship analysis**. Kinship analysis as it stands now is in use as described earlier, to verify immediate first generation family members (DNA STR cross reference between immediate family, siblings and parent-child only, high probability established). With the use of SNP markers and genomic analysis, the analysis moves into highly probable associations among cousins, uncles, nephews/nieces and along paternal and maternal lineage.[50] This analysis opens up opportunities to relate individuals involved in security events with extended family and provides an opportunity for lead development when working back through familial communities of interests and regions. This capability also expands the scope of potential profiling, with attendant ethical and policy implications, to include potential profiles involving sub- tribal affiliations, sub-ethnic characterization, and clan level evaluation of a suspect's possible linkages.

Third, similar to extended kinship analysis, is a potential application in lead generation called **surname inference**. Though immature and demonstrated from commercial genome scans uploaded in popular online genealogy sites, one Massachusetts Institute of Technology (MIT) professor was able to accurately predict a Surname associated with specific DNA samples from machine based datasets and genetic pattern matching in roughly 12% of the

cases, but much higher when working with male DNA and when birth state and dates are included.[51] The research was conducted using public, free-of-charge genetic genealogy databases and their built in search engines. Surname inference, while still in limited in reliability, could yield great benefit to the Security and Law Enforcement communities, particularly when dealing with latent derived DNA from incidents and sites.

Fourth, the use of SNP analysis exposes the underlying genomic markers to reveal likely externally visible characteristics (EVCs), called **phenotypes.** The EVCs include sex, hair and eye color, but also has potential to characterize the positions of ears and noses, address height probability, and even estimate basic facial structure).[52] This is known as one's phenotype, and can be used for physical profiling, and appearance sketches, especially if coupled with advanced software to generate likenesses or physical characterization of suspects based on DNA found on scene at security related sites of interest.

The fifth application of SNP exploitation is in **bio-geographic ancestry** characterization from genomic information. In this application, the genomic markers are analyzed and compared to other genomes common to very specific regions of the world. Using pattern matching algorithms, sample DNA SNPs can be analyzed to determine probable origin of the suspect individual and relates to specific demographics, such as Northern European, South Asian, Asian, Pacific Islanders, Hispanic, etc. As the data sets mature and the machine learning, it can be expected that bio-geographic ancestry exploitation would also further intelligence lead generation, human trait analysis, and threat network development. While this application does not directly identify an individual, it does assist in the analysis of forensically derived DNA in support of suspect screening and broader threat network analysis.

The sixth research area for DNA SNP analysis with potential application for national security is **epigenome activity analysis**. This analysis could provide information on changes in genome structure, based on chemical modifications that can be caused by contact with specific chemicals or organic materials, environmental factors, foods, lifestyles and other individualized

activity based phenomenon. The assessed causes of change in the epigenetic markers could help identify individuals likely to have handled certain chemical, biological or radiological precursor substances associated with weapons of mass destruction (WMD). Similarly, the change to the markers can identify activity associated with regular exposure drug manufacturing, explosives, and certain identifiable regions of the world through organic material signatures and their effect on the human genome.

And lastly, another element of information value is present within information not on the human DNA of the suspect individual, but of the microbial DNA found in tandem with the suspects DNA, as they live on and within the individual's body. This microbial analysis, called **metagenomics**, is performed on DNA collected concurrently with the human's reference sample or latent DNA sample. In the future, metagenomics could also provide a level of information surrounding the probable previous geographic locations of an individual and the individual's likely activities- from contact with bacteria and other microbial organisms found in foods, water, and pesticides, but also with precursor chemicals and materials used in manufacturing weapons of mass destruction, drugs, and explosives. These microbes are "co-travelers" with every person as there are more non-human microbial cells on the human body than there are human cells.

Next Generation SNP DNA Biometric Use Cases. The premise in the use case scenarios that follow is based on the idea that once a DNA SNP sample is derived, the tools and applications which could be applied are all viable. Said a different way, once the DNA SNP region is captured and the genomics are exposed and entered into the biometric system, the full range of techniques as described above could be employed to exploit the information and intelligence value of the sample for national security use. Primary cases are described below:

- **Sensitive Site Exploitation.**[53] Once a terrorism related event occurs or an operational action is taken against individuals associated with terrorist, drug, WMD, or other networks of national security interest, the opportunity for

exploitation of all related materials and details surrounding the event or site presents itself. The opportunity to gain insight from the many analytic and investigative techniques run the gamut from on-site interviews of witnesses, follow on detainee questioning, forensic evidence collection and exploitation, exploitation of digital media and documents found on-site, as well as other link analysis techniques applied once positive or suspected linkages are established.

Most operational teams conducting Sensitive Site Exploitation (SSE) do so with a view on collecting forensic evidence and intelligence for future use. Information extracted from the exploitation processes establish the identity or background of individuals found on or in the immediate vicinity of the site. These teams carry equipment sets specially developed to conduct a full range of intelligence and criminal investigative operations at the site. Team members should be fully trained and vetted for the collection of DNA and other biometrics, especially when the biometrics are potentially used in prosecution and network development.[54] The NG DNA exploitation at a site could reveal the presence of network related individuals on site, previously on site and those individuals not on site but previously associated with materials, objects, documents and illicit items found on site. The use of NG DNA exploitation could significantly enhances the information value of SSE.

Through **mixture analysis**, a confirmation of a suspect's reference sample located within a complex latent mixture sample can be made. This is a step forward from current capabilities, with great merit for both the law enforcement and national security community, when thinking about its potential in analyzing weapons involved in violent acts, drug or WMD materials and even documents and media taken from sensitive sites.

As the science and technology progresses, deconvolved mixtures would allow for individual profile extraction and analysis. Deconvolution would then enable cross-checking for match against known and unknown individuals-verified as 1:1 match, N:N, and N:1 matches. In other cases, the latent sample remains unknown but is entered into the dataset, along with SSE contextual information. A match to previous SSE or other latent DNA samples through deconvolution would help confirm linkages of involvement across a serial of terrorist, criminal or other illicit activities.

The virtue of entering the DNA SNP information is enabling a deeper set of network development analytics and a richer set of tipping and cueing across the national security enterprise. In the mixture analysis example, a capability emerges to create the capability to match unknown (but still interesting) individuals to previous events, sites, and locations. In turn, this greatly aids the network analysis process to fully develop a network profile in terms of linkages across individuals, locations, materials, facilities and events.

Through the use of **phenotype analysis**, a visual characteristic can be discerned and a visually useful profile can be established. This “computer generated sketch” of EVC subsets could be shared rapidly across US and partner communities, especially valuable when additional contextual information further enriches the qualities of the sketch. With the ability to perform likeness generation comes a screening capability, particularly useful in ports of entry, checkpoint operations, event access screening, public awareness/safety messages, etc. Though this clearly does not confirm identity, nor should it, it does provide a machine-based ability to generate results that complement manual sketches which are dependent on witness or informant memory (potentially more objective and certainly faster).

Additional application of **extended kinship analysis** allows for deeper level investigation in establishing linkages to previously detained or enrolled individuals related to an unknown individual based on DNA. First Generation DNA matching has been used in specific instances in Afghanistan, whereby an unknown subject's DNA was recovered from components of an Improvised Explosive Devise (IED) and was subsequently assessed to be a relative match to a known individual (previous enrollee-the father). Because the enrollment processes (reference samples) also provide contextual features such as name, residence or village location, and other identification or biographic features, etc., the ability to go from unknown to known improves dramatically in these circumstances. The ability to detain the individual described above, with an Afghan court arrest warrant, was generated from parent-child DNA analysis and a simple questioning of the family and neighbors as to the whereabouts of the son. Once the son was found, he was enrolled in the DNA database and a match was subsequently confirmed between him and the IED latent DNA evidence. With extended kinship, the ability to go from an unknown individual's DNA to a range of likely family relationships and locations will aid lead generation, search, and investigation significantly.

Bio-geographic ancestry analysis also can be directly integrated from latent SNP DNA extracted from SSE operations, and furthers the capability of analysts to develop intelligence and criminal leads for unknown individuals. Though bio-geographic ancestry characterization, additional information is derived and can be fused with other contextual data related to the SSE, but also directly integrated with the phenotype and extended kinship related markers to even more fully characterize and profile the unknown suspect. Additionally, the range of individual ancestral backgrounds of suspects involved in a security

incident can significantly advance the network development process, exploit additional features from mixture analysis and lead to a terror cell level or sub-network profile of associated related individuals.

- **Countering WMD, Drug and Weapons Trafficking Networks.** Within the added capability of **epigenome analysis** and attendant **microbial analysis**, a broader capability emerges to assess prior activity and association with materials, chemicals and organic substances, especially important when attempting to develop WMD, drug and explosive related network trafficking or WMD precursor handling by suspect individuals. While the epigenome and microbial activity analysis could be relevant to the previous use case as an SSE and network development tool, it is even more viable as a potential tool to identify individuals involved with WMD, drugs and explosives at the primary level. The individuals would likely have clear genomic marker changes based on exposure to known substances and this trait would show itself in both latent DNA samples ad direct reference samples. This is particularly important in national security operations working to counter chemical, biological and radiological WMD proliferation. These are capabilities that fundamentally identify and characterize individuals involved in high threat/high interest networks.

Identity Resolution as a component of 21st Century National Security[55] The decentralization, increased access to lethal means and the rise of fully networked empowered actors create significant challenges to the nation's security system. No longer do we deem our nation secure due to two oceans on our flanks and secure and friendly nations to our north and south. Our military capability and interagency intelligence capabilities can no longer simply focus on the rival state military formations and weapons systems. The world has changed.

The threats today come from state and non-state actors capable of moving themselves, weapon components (to include potential WMD and high order explosive components) and

financial resources via commercial or industrial mechanisms. Individuals can remain connected through the worldwide web and cellular based smart phones yet remain operationally dispersed. Operational planning, training and rehearsals can be conducted online via gaming venues and video postings. Knowhow and resourceful improvisation to create mass effects are hallmarks of the emerging threat. Anonymity and the ability to hide in plain site are operational and strategic assets for these threat actors and networks.

In the past, less than 30 years ago, the nation devoted great treasure toward intelligence capability, weapons, applied research and development, and ready, standing forces to counter the Soviet threat. We focused on enemy objects and related organizations. It was a standard practice to maintain vigilance on the status of Soviet bomber fleets, submarines, armored divisions, mobile rocket deployments and state communications – military orders of battle. We felt that a lack of vigilance would lead to a chance of surprise, and a surprise (however small or great of a probability of actual US-Soviet conflict) could realistically result is a catastrophic failure for the nation. Today, the threats are not simply found in the fabric of the nation state, but in the sinews and networks of non-state actors and individuals – requiring the shift from orders of battle to the human social networks that constitute a national security threat.

No longer are we primarily concerned about nuclear confrontation and massive conventional force conflict, but we are increasingly concerned about a repeat of September 11, 2001. A repeat that could conceivably involve WMDs or other weapons of mass effect aimed at undermining confidence in our government's capacity to protect the homeland or our interests abroad. No longer are the objects of war tied to state based military organizations – highly lethal capabilities are now accessible to individuals empowered by information and social networks. The question is, if the threats of 30 years ago were dissuaded and countered by our own massive capacity to respond, especially as a deterrence model, then why shouldn't we similarly investing in capabilities to advance our security posture to defeat and deconstruct our current networked threats at the individual or granular level of organization. It will require a

capability to both resolve and assure identity, expose hidden threat actors, and maintain a repository of highly refined threat event related data.

Section Four- Recommendations for Adjustment or Creation of Policy[56]

Clearly there is a need to address policy, civil liberties and ethics as Research and Development investments are made and technical advances provide opportunities in DNA biometrics for national security. To be clear, these recommendations and the thrust of this paper is not advocating for a widespread DNA capture and catalogue of DNA from non-US/foreign persons. Biometrics and Forensic advances are not going away, and the science will progress. Biometrics is a class of information whose use cannot be controlled simply by USG policy – as the capability is available to other nations and to our adversaries. It is also not a given that the advances and application will come from US commercial efforts, as the scientific and technologic communities involved in genomic exploitation are worldwide and are not subject to US law, oversight or American ethical consideration for use. Progress in next generation biometrics will be made whether the US Government leads the effort or not. The emphasis here is to ensure the USG is not surprised, our own national security operations are protected, and the advances in the field of biometrics lead produce continued advantage for US national security. It is imperative that the USG maintains an informed and clear understanding of the science and potential applications of these advances, establishing leadership in the advancement and adaptation of the technologies for national security, rather than be an interested bystander or take a reactionary role such as “watchful waiting.” We must ensure the people of the US and our communities of interest are clear on the science, address the inherent privacy and civil rights issues surrounding the use of biometrics, and that the proper policies are adopted and adapted concurrently with operational advancement. Work must be done to preserve the value of these biometric capability advances as a means of maintaining our global operations posture for national security.

Recommendations for Policy.

- **Ready the DoD for the Bioinformatics Big Data Problem.** The genomic sequencing applications for national security under the NGGA/NG DNA advancements will generate huge datasets that are currently not mapped sufficiently in current architectures and are not accounted for in terms of IT protocols, processing schemas, or community authorities. There are structures in place for biometrics which could, and should be, pursued in light of these advances and the scope, scale, and volumes necessary to enable forward operational access and latency requirements.
- **Mandate and maintain DNA Database access oversight**. As CODIS or another DNA database matures to accommodate mobile DNA collection and SNP data ingest, the distributed data and access protocols should be clearly established. Currently, the FBI has no intent to adjust the architecture of CODIS to expand beyond STR profiles. If a CODIS expansion or alternative DNA database were established for NGGA/NG DNA, direct access should be very limited with credential verification. Portals of entry will be widely expanded to handheld devices, different from the current lab entry processes today. Similar to fingerprint booking where individual police booking procedures upload, DNA sample (latent and reference) uploads will occur regularly from distributed users. Oversight for database access and upload should involve only credentialed or verified, registered individuals with authentication, repudiation, and metatagging embedded in each transaction.
- **Require a full context report to be filed with each DNA upload.** Context should be required for DNA ingest/upload, but remain controlled and limited in association with the DNA profiles and datasets. Context reporting will assist in discovery and fusion for intelligence and lead generation, as well as reduce

concerns of falsification of evidence and tampering. Contextual reporting would likely increase processing time, but it is important for intelligence analysis and network development activities. DNA (as well as other biometrics) is fast becoming another tool for all-source intelligence and a key component of intelligence fusion.

- **Require certification for sample collection related to SNP Genome Analysis and establish control protocols**. Mitigate concerns or allegations of planting DNA and synthetic DNA generation, awareness of DNA masking and evidence tampering, while reassuring the public that civil liberty and privacy are being protected.
- **DNA upload and retention of DNA from US Citizens/US Persons should be controlled and only authorized through a warrant process.** Much like the FISA laws and Title 50 Intelligence Collection oversight requirements for US Government agencies as related to US citizens and persons, a similar policy and law should be established for DNA processing and after the fact procedures when involving US citizens/persons. This may include procedures and automated information destruction of DNA based information when found to be entered in error or when found to be incidental to collection but cleared of association with events and foreign persons of interest.
- **Establish DNA Sharing Mechanisms and Overall Policy with Other Nations.** The basis for sharing DNA information should be in US interests and serve to advance US national security, while also assisting in partner efforts to deal with their own 21st century security requirements. Clear policy guidelines should over circumstances of sharing, the sharing of DNA information on US persons (not recommended) and of partner nations citizens (limited circumstances) and on third party individuals (likely the norm to emerge).

- **Interagency Sharing.** Establish clear sharing protocols and guidelines for interagency access and use of DNA SNP information for their own uses.
- **Establish Training Requirements**. All individuals that are involved in handling DNA latent and reference samples at the point of network ingestion and upload should have training on DNA handling, device operations, policy, legal authorities and responsibilities.
- **Education on Use Cases and basics of DNA biometric science.** For the user community, policy and legal communities involved with national security and biometric capabilities.

Section Five- Summary and Conclusion

This paper presented a review of the current primary biometric modalities and evaluated the likelihood that any one of the modalities, given current science and technology trends, could achieve a significant breakthrough within the next five to ten years. The national security community has an established need for reliable biometric modalities, capable of working across a global landscape, with precision, speed and accuracy. These national security interests changed by becoming more complex and decentralized since the end of the Cold War. Denying anonymity, countering threat networks of human actors and Super-Empowered Individuals capable of lethal, mass casualty producing effect, changes the tools required for successful intelligence and security operations.

After evaluating the current modalities, the Next Generation Genomic Analysis (NGGA) and Next Generation DNA biometrics capability stood out as having the greatest promise for meeting 21st Century national security requirements, in terms of the biometric component. The application of biometrics in overseas combat, counter-terrorism, counter-proliferation, and counter-network operations is valuable and should be considered another advantage for the nation. When considering the current US policies, laws, and sharing directives in light of the advances in DNA based biometrics, gaps stand out. If these gaps are not addressed, and USG

policies, investment into applied research and development may hinder the value and applicability of these advantages in defeating and deterring 21st Century adversaries.

This paper established a series of feasible scenarios or "use cases" for consideration in context of the current DNA modality with a Rapid DNA analytic capability and NGGA/NG DNA potential advances, specifically in national security operations. **Five Rapid DNA use cases** stood out- **Incident witness and suspect enrollment, forensic exploitation and match; Border screening and immigrant analysis; Watchlist screening; Maritime Interdiction and Screening.** In terms **Next Generation Genomic Analysis (NGGA) and Next Generation DNA (NG DNA) use cases**, offering information for national security well beyond identity resolution, there are **two main use cases** fall into the categories of **Sensitive Site Exploitation (SSE)** and **Counter-WMD, Drug and Weapon Trafficking Networks.** With advances in NGGA/NG DNA, the capabilities of DNA biometrics expand to **mixture analysis, extended kinship analysis, surname inference, phenotype analysis of externally visible characteristics, bio-geographic ancestry, epigenome activity analysis and related microbial analysis** (**metagenomics)**.

This paper proposes eight specific recommendations to address policy gaps and other community level changes required to fully leverage NGGA/NG DNA future capabilities. The recommendations are: **Ready the DoD for the Bioinformatics Big Data Problem; Mandate and maintain Next Generation DNA dataset and database access oversight**; **Require a full context report to be filed with each DNA upload; Require certification for sample collection related to SNP Genome Analysis and establish control protocols**; **Control DNA upload and retention of DNA from US Citizens/US Persons and only authorize through a warrant process; Establish a DNA Sharing mechanisms and overall policy with other nations; Establish protocols for Interagency Sharing; Establish training requirements**; **Promote education on Use Cases and basics of DNA biometric science.**

Opportunities and recommendations for further research following from this paper are in continued development of use cases into full concepts of operation and technology integration, reviewing and evaluating policy adjustments and in the evaluation of a community NGGA/NG DNA Information Architecture that would fully support the potential advances in DNA biometrics outlined in this paper.

Acknowledgements: The author would like to thank the subject matter experts and senior biometrics community leaders for their valuable time and substantial input to this project. I also put on record my sincere appreciation to Dr. Paula Collins and Dr. Jim Harper from MIT Lincoln Laboratory for their time and patience, insightful comments, and critical review of the technical aspects of this paper. Mr. Ed Wack, as the leader of MIT Lincoln Lab's Group 48 (Bio-engineering) of has also been a superb project mentor and his steady guidance to me as I pursued the topic was a key element in my ability to work through the drafts and bring the paper to completion. Any errors in this paper or its conclusions remain with the author.

Endnotes

[1] Biometrics Community accepted definition of Biometrics: A general term used alternatively to describe a characteristic or a process. As a characteristic: The measure of a biological (anatomical and physiological) and/or behavioral biometric characteristic that can be used for automated recognition. As a process: Automated methods of recognizing an individual based on the measure of biological (anatomical or physiological) and/or behavioral biometric characteristics. Source is from the National Science and Technology Council (NSTC) Subcommittee on Biometrics. The NSTC developed this definition in order to standardize the reference. The NSTC Biometric Glossary is available at *The Biometrics.Gov Homepage*, www.biometrics.gov (accessed March16, 2013). The site also maintains a broader set of references in a document called "Biometrics Foundational Documents" at http://www.biometrics.gov/ReferenceRoom/Introduction.aspx.

[2] This is the author's conservative estimate through compiled research documents and attendance at the Biometric Consortium Conference in September, 2012.

[3] According to the November 2011 market research firm Global Industry Analysis report, total global investment across all sectors of biometric use (health, security, public services, law enforcement, private security and identity management) will reach nearly $16.5B, indicating a push in corporate and non-governmental sector investment for identity management and as well as a continued investment in security related US Government investment from the Departments of Defense (DoD), Justice (DoJ), and Homeland Security (DHS). See Homeland Security Newswire article "Strong Growth in Biometrics Industry Projected," *Homeland Security News Wire*, November 17, 2011, http://www.homelandsecuritynewswire.com/strong-growth-biometrics-industry-projected (accessed February 07, 2013), highlighting the 2012-2017 biometric industry market forecast from the market research firm Global Industry Analysts (GIA). It is not likely that the current level of US DoD investment in biometrics will remain as high as their peak in the 2006-2010 timeframe, which was largely tied to Overseas Contingency Operations Funding for Afghanistan and Iraq rather than program base funding. Comments on funding declines in DoD from personal interview with US DoD senior biometrics leader.

[4] See Amy Gutmann, *Privacy and Progress in Whole Genome Sequencing*, October 2012, Washington, DC, (Washington, DC: The Presidential Commission for the Study of Bioethical Issues, October 2012), see especially the Introduction, Chapter 2 (Policy and Governance), and Chapter 3 (Analysis and Recommendations), available at http://bioethics.gov/cms/node/764.

[5] The term Super Empowered Individual (SEI) was first coined by Thomas Freidman in his book 2002 book *Longitudes and Attitudes, Exploring the World After September 11*, and addresses the rise of the individual's impact on a globalized, technologically connected world, especially as power structures and capability move from the Nation State to the Non- State Organizations and networked individuals – the shift from Super Powers to Super Empowered Individuals. Rather than a definition solely associated with a single author, the SEI references are now common and continues to be addressed in official documents, proclaiming the rising impact individuals can make in the 21st Century. These individuals are Super Empowered due to the networks they build or associate with, the speed and quality of information transfer, their access to resources, the credibility they garner, and the resultant power they can leverage across social-economic-political systems. See Thomas Friedman, 'Prologue: The Super-Story,' Chapter in *Longitudes and Attitudes: Exploring the World After September 2011* (New York: Farrar, Straus & Giroux, 2002), 3-6. Excerpt available online at: http://www.thomaslfriedman.com/bookshelf/longitudes-and-attitudes/prologue; see also both the US National Intelligence Council's *Global Trends 2030: Alternative Worlds* (Washington, DC: National Intelligence Council, 2012), 8-14, available at http://www.dni.gov/index.php/about/organization/national-intelligence-council-global-trends and the Atlantic Council's complementary publication *Envisioning 2030: US Strategy for a Post-Western World* (Washington, DC: The Brent Scowcroft Center on International Security), 6, available at http://www.acus.org/publication/envisioning-2030-us-strategy-post-western-world.

[6] According to the National Research Council's authoritative 2010 report on Biometrics, the definition of a biometric modality is the combination of a biometric trait, sensor type, and algorithms for extracting and processing the digital representations of the trait. When any two of these three constituents differ from one system to the next, the systems are said to have different modalities. National Research Council - Whither Biometrics Committee, *Biometrics*

Recognition: Challenges and Opportunities (Washington, DC: National Academies Press, 2010), 31. Available at http://www.nap.edu/catalog.php?record_id=12720.

[7] Ibid, 15-52. The author draws heavily on the council's work in the section one overview (Introduction and Fundamental Concepts).

[8] FBI estimates DNA has a 1 in 1 billion or greater statistical chance of random false match rate error, from use of the 13 loci in the standard STR analysis process, see "DNA Evidence: Basics of Analyzing," http://www.nij.gov/topics/forensics/evidence/dna/basics/analyzing.htm, (accessed March 15, 2013) from The National Institute of Justice Homepage. In recent years, challenges have emerged as to the confidence in fingerprint analysis and the iris, due to the affect of aging on the iris. See Samuel P. Fenker and Kevin W. Bowyer, *Analysis of Template Aging in Iris Biometrics,* paper presented at the IEEE Computer Science Community Biometrics Workshop, June 17, 2012, and the National Research Council's Committee on Identifying the Needs of the Forensic Sciences Community report *Strengthening Forensic Science in the United States: A Path Forward* (Washington, DC: National Research Council, 2009), 7, which found systemic problems within specific biometric systems and "with the exception of nuclear DNA analysis, no forensic method has been rigorously shown to be able to consistently, and with a high degree of certainty, demonstrate a connection between evidence and a specific individual or source."

[9] For example, the optimal biometric enrollment in combat zones for security application and intelligence use is the "10+2+1+1" shorthand reference. This allows for biometric fusion of a single individual's biometrics, in case of future "hits" or verification requirements; there are multiple reference samples available to identify the person. The 10+2+1+1 refers to the enrollment of all 10 fingerprints, both iris's, one frontal facial photograph and a DNA buccal cell swab. Operating forces are provided field collection and enrollment capabilities to include forensic kits, handheld enrollment devices, and access to biometric watch lists.

[10] Author's own experience in Afghanistan, working with tactical military units and the Biometrics Task Force-Afghanistan, as well as participating in numerous Biometric Community subject matter expert discussions on the subject.

[11] **Non-Contact** refers to the ability to collect the biometric sample without physically touching the individual, such as recovering a latent fingerprint or DNA sample, but also from conducting an iris scan from a device close to the individual but without touching. **Stand-Off** is a different class of Non-Contact, normally from a collection devise at a greater distance from the individual in real time, such as cameras designed to collect facial features or other behavioral characteristics, often without the subject being aware of the collection device.

[12] A **Cooperative** user is an individual that willingly provides his or her biometric to the biometric system for capture. A **Non-Cooperative** user is an individual who is not aware that a biometric sample is being collected. An **Uncooperative** user is an individual who actively tries to deny the capture of his or her biometric data. Definitions are from the National Science and Technology Council's Subcommittee on Biometrics and Identity Management report *The National Biometrics Challenge*, (Washington, DC: Executive Office of the President of the United States, September 2011), 5. Available at www.**biometrics**.gov/nstc/publications.aspx.

[13] In the normal field operating environment, collection must occur in a wide variety of conditions. The factors of weather, temperature, crowds, public locations, limited lighting, lack

of electricity, lack of security, etc., all affect the potential for the collection and quality enrollment of biometric data.

[14] Rapid is defined as less than two hours from time of sample to the extraction and coding/digitization of the biometric information contained in the sample for comparison or initial ingest into a standardized database. Ease of use should be assessed by simply making equipment or tools that can be used by normal operational field personnel with a basic fundamental level of training on the device and without the requirement for specialized operators or technicians at the point of collection and initial exploitation. Within the next five years, the technologies will advance and will likely provide the capability to produce STR and SNP DNA profiles in less than one hour using portable devices in field conditions.

[15] The need for data into an enterprise architecture means the data can be entered and extracted via secure/encrypted access to the World Wide Web (WWW), a Virtual Private Network, or a Cloud Based infrastructure, via 3G/4G cellular networks, Public Switched Telephone (PST), or satellite communication (SATCOM), in order to access the authoritative biometric database.

[16] The matching process should support a **known to known (1:1)**, **unknown to known (N:1)**, **unknown to unknown (N:N)**, and **known to unknown (1:N)** set of conditions. A **1:1** match means verification between a database sample and a reference sample, when directly comparing the two. An unknown to known is a **N:1** match, whereby an unknown individual's biometric sample is compared to a database of known biometrics and a match is identified (an example would be a DNA latent sample found at a crime scene and the suspect is unknown, but the CODIS database contains a matching DNA sample with a known felon). An unknown to unknown is an **N:N** comparison, whereby an unknown biometric from latent collection is matched to another biometric in the database, but the individuals identity remains unknown (this example frequently occurs in the latent collection of battlefield forensic exploitation, whereby latent fingerprints or DNA is recovered from an IED or terrorist related facility, yet the actual identity is unknown, and a previously enrolled unknown biometric produces a match. We can then confirm the same individual was present in both cases, yet the identity remains unknown. In this case, lead generation and further analysis can provide clues to narrow down the likely individuals, allowing for an action to conduct a deliberate biometric reference sample enrollment to confirm the individual). An **1:N** match means a known biometric (reference sample) is compared to a database with an unknown individual's biometrics and a match occurs (this also occurs frequently in battlefield conditions whereby a previously enrolled, yet unknown individual's latent biometrics are pulled from a site or IED related material, and after the fact an individual is enrolled and the unknown becomes known.

[17] The advances in DNA sequencing would support lead generation based on phenotype visible trait analysis, bio-geographic ancestry, epigenomic activity analysis and extended kinship analysis. None of these techniques by themselves would confirm identity but each of them could generate leads on suspects or persons of interest for intelligence and law enforcement. Each of these capabilities is feasible for application in national security use cases within the next five to 10 years.

[18] The author conducted over 20 of interviews, email exchanges, and follow-up interviews from August 2012 to March 2013 with a number of leading scientists and biometric community leaders. Interviews included: John Boyd, Director of Biometrics and Forensics, Office of the Secretary of Defense, Assistant Secretary of Defense (Research and Engineering) [initial

interview Tampa, FL, September 18, 2012]; Dr. Joseph Campbell, Associate Group Leader, Human Language Technology, MIT Lincoln Laboratory and Committee Member, National Research Council (Biometrics Committee); Dr. James Harper, Assistant Group Leader, Bioengineering Systems and Technologies MIT Lincoln Laboratory; Jon Lazar, Biometrics Program lead, Office of the Secretary of Defense, Assistant Secretary of Defense (Research and Engineering) [initial interview Tampa, FL, September, 18, 2012]; Dr. James Loudermilk, Senior Level Technologist, Federal Bureau of Investigation, Science & Technology Branch [initial interview Tampa, FL, September 19, 2012]; Dr. Christopher Miles, Program Manager, Department of Homeland Security, Science and Technology Directorate [initial interview Tampa, FL, September 19, 2012]; Mr. Al Miller, Office of the Under Secretary of Defense for Policy (Biometrics) [initial meeting and research topic overview Tampa, FL, September 19, 2012]; Christopher Munn, Biometrics lead, Department of Defense, Office of the Undersecretary of Defense - Intelligence [initial interview Tampa, FL, September 19, 2012], Dr. Paula A. Collins, Technical Staff, Bioengineering Systems and Technologies MIT Lincoln Laboratory; Mr. Peter Verga, Chief of Staff, Under Secretary of Defense - Policy [initial meeting and research topic overview Tampa, FL September 18, 2012], Mr. Edward Wack, Group Leader, Bioengineering Systems and Technologies MIT Lincoln Laboratory. Any mistakes made or misinterpretations of the Subject matter Experts opinions and insight on the topic are the author's alone. The author also attended the 2012 Biometrics Consortium Conference (BCC), considered to be the primary annual event for the biometrics research, commercial policy and user communities. The BCC covered the current state of biometrics science and applications, and made future projections across current and emerging modalities. Conference subjects and presentations are available online at http://www.biometrics.org/conferences.php. Additionally, the author participated in numerous technical reviews of biometric technologies at the MIT Lincoln Laboratory and has direct experience with multimodal biometrics in field conditions in Afghanistan for US, Coalition and Partner security and intelligence use.

[19] The primary biometrics evaluated in this paper are in use today by DoD, HLS, and the DoJ. Secondary or alternative "other" categories as those biometrics that are relatively new, lack scientific statistical confidence, or otherwise are immature in their application at scale.

[20] The following modalities were initially considered and then removed from the evaluation: **Gait** - immature and does not allow for identity resolution and there are no prospects for significant advances in the modality; **Hand Geometry** - while increasing in use and maintaining an good track record for application in access control, the use of hand geometry is insufficient and impractical for use in a law enforcement or intelligence role. Other emerging **"Soft Biometrics"**- such as **Scars and Tattoos** are being explored in the Department of Justice but are not considered sufficient for prosecution or mature enough to be considered a full biometric, and are not suitable for national security application, other than some potential as a lead generation physical attribute.

[21] John M. Butler, *Fundamentals of Forensic DNA Typing* (Burlington, MA: Academic Press, 2010), 4-7.

[22] **STR DNA analysis** refers to a common, internationally used DNA processing technique which compares variations (polymorphisms) of short repeated sequences the base nucleotides (composed of polymer codes A-adenine, C-cytosine, G-guanine, or T-thymine) within a sample strand of DNA. The number of times the particular A-C-G-T sequence variation occurs within the DNA segment varies between individuals. The physical position of the marker nucleotide is called the *loci*. Law enforcement and judicial system standard practice is to analyze 13 to 16

loci for comparison of DNA samples (creating a DNA profile) to determine a match. The likelihood of an STR profile falsely matching another random sample to someone unrelated to the reference sample is 1 in 1 billion. For close relatives the match probability drops significantly but remains statistically unlikely (a siblings random match probability is 1 in 10,000, while a first cousin random match probability is 1 in 100 million). Additionally, the STR loci are considered to be the non-genetically coded segments of the DNA sequence within a specific chromosome, and therefore does not provide genetically useful information for use in genetic analysis for health care purposes, genetic characterization or reveal any other genetic code related information. The polymorphisms within the short tandem sequence string are therefore useful in verifying identity match as well as for paternity testing, as the STR used is genetically inherited. See Butler, *Fundamentals of Forensic DNA Typing,* as the definitive guide on DNA analysis and statistical confidence reference for DNA profile analysis. For Random Matching Probability table, see page 250.

[23] Another DNA analysis technique commonly used for establishing maternal parentage linkage and in the identity analysis for remains such as POW/MIA remains and other situations involving the remains of persons in a degraded condition is Mitochondrial DNA analysis.

[24] Ibid, 342-348. **SNP DNA analysis** refers to the analysis of both the non-coding, the intergenic, and/or and the genetic coding portions of a single DNA nucleotide (the individual polymers A, C, G, or T), analyzing polymorphisms in multiple markers simultaneously. The SNP analysis draws on the scientific breakthroughs from the genome mapping efforts associated with the Human Genome Project. SNP analysis can be used for identity verification, ancestral information, extended kinship/lineage, and phenotype (traits and characterization) as well as supporting the ability to identify genetic changes through mutation as the genes replicate themselves, as used in toxicology and disease pathology studies.

[25] Susan Walsh et al, "The HIrisPlex System for Simultaneous Prediction of Hair and Eye Colour from DNA," *Forensic Science International: Genetics* 7, (July 2012): 98–115. This paper establishes the capability for predictive use of latently collected DNA markers to establish leads from hair and eye color, with additional characteristics being ethnic descent/ancestry, capable of genetically inferring, for instance, a northern European male with black hair and brown eyes from south Asian with black hair and brown eyes. While the science advances, it is also likely that additional characteristics such as shapes of the nose, placement of the earlobe, separation distance of the eyes, height parameters, etc., could be inferred as well. Once the genome markers are understood and found reliable for predicting physically visible traits, it is also likely that a computer aided design program could generate a basic likeness of an individual based on these traits.

[26] The digital file is an algorithm converting the scanned actual finger or inked image fingerprint into unique digital features – the patterns or minutia in everyone's individual fingertip.

[27] See *The Department of Homeland Defense Homepage,* US-VISIT program http://www.dhs.gov/us-visit-resources-and-materials (accessed March 19, 2013) for a description of the current technical standards for the US-VISIT program. There is an intent to also incorporate additional biometric modalities- palm print, iris and DNA, as outlined in Department of Homeland Security, *Biometric Standards: Requirements for US-VISIT* (Washington, DC: Department of Homeland Defense, March 15, 2010) iii. The European Union (EU) also uses a fingerprint system for political asylum seekers, illegal immigrants and refugees

known as the EU's EURODAC System. For additional information on EURODAC, see http://www.edps.europa.eu/EDPSWEB/edps/EDPS

[28] Dr. Kevin Bowyer, "State of the Art in Iris Recognition," briefing slides and author notes, Tampa, Florida, Biometrics Consortium Conference, September 18, 2012. See also previous reference number 8 - Fenker and Bowyer's IEEE Conference paper, 2012, on the Iris Aging.

[29] Speech patterns with one's supervisor and work colleagues or with a loan officer likely would be different than when speaking with family or hometown friends in an informal environment, to the extent even accent and comprehensive dialect could change.

[30] This table represents the basic qualities of each of the modalities reviewed in this research project. Qualities such a High, Moderate, Low are derived from literature reviews, SME interviews and similar tabular assessments located in the Defense Science Board's 2007 Task Force Report on Defense Biometrics, Appendix 0 – Biometrics Modality Matrix located at http://www.acq.osd.mil/dsb/reports/2007-03-Defense_Biometrics_Program.xls. The evaluation of incremental advances on the non-DNA biometric modalities is based on interviews and presentations at the 2012 Biometrics Consortium Conference and a review of other literature. This evaluation is by the author and does not imply there are not potential breakthroughs in other biometrics in terms of novel collection techniques, processing power, or systems engineering, but the nature of the biometric is unlikely to significantly change in fundamental over the next five to ten years.

[31] See the National Institute of Health - National Human Genome Research Institute Homepage at http://www.genome.gov/ (accessed March 19, 2013).

[32] For a complete copy of NSPD-59/HSPD-24, as well as a full review of the US Government's approach to establishing interoperability and sharing within the field of biometrics for law enforcement, national security and identity management, see the National Science and Technology Council (NSTC) Subcommittee on Biometrics and Identity Management report "NSTC Policy for Enabling the Development, Adoption, and Use of Biometric Standards," (Washington, DC: National Academy of Science, September 7, 2007). See also the NSTC report "Biometrics in Government Post-9/11: Advancing Science, Enhancing Operations, August 2008. The fact that neither of these document address or account for DNA as a biometric is telling, and further indicates a gap for policy and law as it applies to DNA genetic exploitation for national security.

[33] NSTC, Biometrics in Post-911, pp 58-59, review of policy - with full HSPD document and hyperlink. For full text of Presidential Order 13388, see https://www.federalregister.gov/**executive-order/13388.pdf** (accessed March 21, 2013).

[34] See PATRIOT ACT full text at http://www.gpo.gov/fdsys/pkg/PLAW-107publ56/pdf/PLAW-107publ56.pdf and DNA Act House Resolution HR 4640, 42 United States Code at *http://www.cbo.gov/publication/12936* (both accessed March 21, 2013).

[35] US law 42 U.S.C. § 14135e(c), available at http://www.gpo.gov/fdsys/pkg/PLAW-106publ546/html/PLAW-106publ546.htm (accessed March 21, 2013).

[36] See the full text of the Health Insurance Portability and Accountability Act (HIPPA) at http://www.gpo.gov/fdsys/pkg/PLAW-104publ191/html/PLAW-104publ191.htm and the Genetic

Information Nondiscrimination Act (GINA) at http://www.govtrack.us/congress/bills/110/hr493/text (both accessed March 21, 2013).

[37] For a full legal review and explanation of biometrics and law, see John D. Woodward, "Biometric Scanning, Law and Policy: Identifying the Concerns—Drafting the Biometric Blueprint," *University of Pittsburg Law Review 59* (Fall 1997); see also Jennifer Lynch, *Special Report on Biometric Data Collection in US Immigrant Communities and Beyond- From Fingerprints to DNA* (Washington, DC: May 2012).

[38] Douglas Shontz, *DNA as Part of Identity Management for the Department of Defense*, (Arlington, VA, RAND Occasional Paper, 2010). The paper addresses a full range of DNA use for DoD and offers clear recommendations for the community. The author focuses on cost-benefit as one criteria for the broad DoD community use of DNA, and recommends against widespread use of DNA collection as a biometric, primarily due to assessed costs of the processing and overall handling in the face of limited use case scenarios. Due to the broader commercial and scientific community's breakthroughs in processing power, integrated chip technologies and a significant decline in the current and projected cost of genomic analysis, the author of this paper believes cost-benefit in established use cases for national security does warrant the R&D investment to mature and deploy NGGA/NGDNA programs to the national security and law enforcement communities of practice.

[39] Ibid, p. 6

[40] Author first-hand experience as a senior US Army intelligence officer in Afghanistan with responsibility for integrating intelligence derived from tactical biometric programs into targeting and security operations.

[41] Shontz, DNA as Part of Identity Management for the Department of Defense, 6-10.

[42] Mr. Edward Wack and Dr. Paula Pomianowski Collins, "Human Identification and Characterization," briefing slides, Lexington, MA, MIT Lincoln Laboratory, December 05, 2012. and Mr. Edward Wack, "Rapid Human DNA Analysis: Accelerated Nuclear DNA Equipment (ANDE)," Cambridge, MA, MIT Security Studies Program, January 23, 2013.

[43] For example, released for lack of immediate evidence.

[44] Dr. Eric Schwoebel, "Genomic Analysis and Human Identification," briefing slides and author notes, Lexington, MA, MIT Lincoln Laboratory, January 9, 2013.

[45] Irma van der Ploeg, Biometric Identification Technologies: Ethical Implications of the Informatization of the Body, Biometric Information Technology Ethics (BITE) Policy Paper no. 1, draft March 05), 2-3, available at http://www.biteproject.org/documents/policy_paper_1_july_version.pdf, and Amy Gutmann, *Privacy and Progress in Whole Genome Sequencing,* 22-27.

[46] Elizabeth Strickland, "The Gene Machine and Me," *IEEE Spectrum*, March 2013, http://spectrum.ieee.org/biomedical/devices/the-gene-machine-and-me (accessed March 16, 2013). See also CBS News, 23andMe Personalized DNA Test Seeks FDA Approval, July 31, 2012, http://www.cbsnews.com/8301-504763_162-57483267-10391704/23andme-personalized-dna-test-seeks-fda-approval/ (accessed March 19, 2012). Both references illustrate the wider

acceptance and use of commercial genome analysis and the decrease in genomic sequencing costs. Some estimates place the costs well below $100 per run in the next five years.

[47] Center for Strategic and International Security (CSIS) U.S. Department of Defense Biometric and Forensic Technology Forum 2012, online conference video available at http://csis.org/event/us-department-defense-biometric-and-forensic-technology-forum.

[48] Irma van der Ploeg, Biometric Identification Technologies: Ethical Implications of the Informatization of the Body, *Biometric Information Technology Ethics (BITE) Policy Paper no. 1*, draft March 05), 2-3, available at http://www.biteproject.org.

[49] Schwoebel, "Genomic Analysis and Human Identification."

[50] Extended kinship analysis is also being conducted in the commercial arena, allowing for individuals to upload DNA profiles of themselves to venues such as Ancestry.com and FamiltreeDNA.com for private sector use. See http://ldna.ancestry.com/ and http://www.familytreedna.com/ for a tutorial and pricing information (as low as $39.00) on DNA analysis for ancestry analysis (both sites accessed on March 21, 2013). and Amy Docker Marcus, "*A Little Digging Unmasks DNA Donor Names*," *Wall Street Journal*, January 17, 2013, available at http://online.wsj.com/article/SB10001424127887323783704578247842499724794.html?mod=WSJ_hpp_MIDDLENexttoWhatsNewsForth (accessed March 21, 2013).

[51] Dr. Yaniv Erlich is the lead researcher for the Surname Inference Project at MITs Whitehead Institute. See Melissa Gymrek et al, "Indentifying Personal Genomes by Surname Inference," *Science*, January 18, 2013, available at http://www.sciencemag.org/content/339/6117/321.full and Amy Docker Marcus, "*A Little Digging Unmasks DNA Donor Names*," *Wall Street Journal*, January 17, 2013, available at http://online.wsj.com/article/SB10001424127887323783704578247842499724794.html?mod=WSJ_hpp_MIDDLENexttoWhatsNewsForth (both articles accessed March 21, 2013).

[52] The uses of phenotype EVCs are found across numerous scientific literature, with cautions that some traits are not purely genetic but are impacted by environmental factors (such as height) and that the phenotypes are not a conclusive factor in identification. Even without the ability to get to identity resolution through EVC phenotype analysis, the uses for intelligence and law enforcement for lead generation and screening is potentially very useful. See Walsh, et al, "The HIrisPlex System for Simultaneous Prediction of Hair and Eye Colour from DNA," and Manfred Kayser and Peter M. Schneider, "DNA-Based Prediction of Human Externally Visible Characteristics on Forensics: Motivations, Scientific Challenges, and Ethical Considerations," *Forensic Science International: Genetics 3*, (June 2009): 154-161.

[53] Sites can be as simple as a vehicle or a campsite, to a hotel room or safehouse, or as complex and sophisticated as a state sponsored chemical or biologic weapon production or storage site. See U.S. Department of the Army, *Site Exploitation Operations*, Army Field Manual FM 3-90.15 (Washington, DC: U.S. Department of the Army, June 2010). Available online at http://armypubsarmypubs.army.mil/doctrine/DR_pubs/dr.../attp3_90x15.pdf.

[54] Teams and individuals should also be fully aware of the potential for concern on the allegations of "planting" evidence or spoofing DNA evidence from synthetic reproduction of DNA samples. The overall circumstance of the incident, details from the site, and other all source

intelligence and evidence should be available for cross reference by investigators when reviewing DNA profiles obtained by site exploitation teams.

[55] This discussion on identity and shifting intelligence emphasis draws on the many insights provided by Mr. Chris Munn, USD-I for Biometrics. Mr. Munn is a leading thinker on identity and the future of intelligence requirements to identify SEIs. In addition to an author interview and follow up conversations with Mr. Munn, he conducted two conference presentations at the BCC Tampa, 2012. Conference slides are available at http://www.biometrics.org/bc2012/presentations/DoD/03%2520Munn%2520BCC%2520Brief%25201040.pdf.

[56] The recommendations made in this paper are informed by reviews of the following: Gutmann, *Privacy and Progress in Whole Genome Sequencing, Ethics in Genome Sequencing*; CSIS's 2012 forum on U.S. Department of Defense Biometric and Forensic Technology; Woodward, "Biometric Scanning, Law and Policy: Identifying the Concerns—Drafting the Biometric Blueprint;" Whither Biometrics Committee of the National Research Council, *Summary of a Workshop on Technology, Policy and Cultural Dimensions of Biometric Systems* (Washington, DC: NRC, 2006); National Science and Technology Council, *Biometrics in Government Post-911: Advancing Science, Enhancing Operations*; Shontz, *DNA as part of Identity Management for the Department of Defense*; Lynch, *Special Report on Biometric Data Collection in US Immigrant Communities and Beyond- From Fingerprints to DNA;* The National Science and Technology Council (NSTC) Subcommittee on Identity Management, *The National Biometrics Challenge* and the NSTC's, *Policy for Enable the Development, Adoption, and Use of Biometric Standards* (Washington, DC: September 7, 2007).